REMARKS

I. Amendments to the Claims

Claims 24-41 and 43-46 are pending and under examination. Applicant amends claims 24, 26, 27, 39-41, 43, and 44 as indicated in the listing of claims. These amendments are supported by Applicant's specification at, for example, page 3, lines 6-34, and page 5, lines 22-30.

II. Final Office Action

Applicant respectfully traverses the rejections set forth in the Final Office Action, wherein the Examiner:

1) objected to Figs. 1, 3, and 5;

2) rejected claims 24-41 and 43-46 under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement; and

3) rejected claims 24-41 and 43-46 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,177,425 ("Ben") in view of U.S. Patent Application Publication No. 2004/0204124 ("Campbell").

III. Response to Rejections

A. Objection to the Drawings

The Office Action, on page 2, stated that "[n]ew corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because figures 1, 3 and 5 do not contain written description to the steps involved." In response, Applicant amends Figs. 1, 3-6, and 7, as reflected in the attached five (5) replacement drawing sheets which contain Figs. 1 and 3-7. Specifically, Applicant adds labels to the blocks in Fig. 1, 3, and 5, and amends the descriptions of step 200 in Fig. 4 to state "Request Access to Sensitive Data," steps 314 and 316 in Fig. 6 to respectively state "Encrypt User Credentials with Encryption Key and Random Vector," and "Store Results of Encryption Procedure and SIM IMSI," and steps 400 and 402 in Fig. 7 to

respectively state "Receive Access Request," and "Connect to SIM." The amendments are supported by Applicant's specification at, for example, page 13, lines 12-13 and 19-27; page 17, lines 32-34; and page 18, lines 3-7 and 20-21. Accordingly, Applicant requests withdrawal of the objection to the drawings and entry of the attached replacement drawing sheets.

B. Rejection under 35 U.S.C. § 112

The Office Action, on page 2, rejected all pending claims under 35 U.S.C. § 112, first paragraph. Specifically, the Office Action stated that the limitation "storing said protected data resources in said remote database in an encrypted format along with said data resources," as recited in claim 24, is not enabled by Applicant's specification. To advance prosecution, and without conceding to the Examiner's rejection, Applicant amends claim 24 to delete "along with said data resources," and similarly amends claim 39. Applicant, thus, respectfully requests withdrawal of the rejection.

C. Rejection under 35 U.S.C. § 103(a)

The Office Action, on page 3, rejected all claims under 35 U.S.C. § 103(a) as being unpatentable over Ben in view of Campbell. Applicant respectfully traverses this rejection because the Final Office Action has not properly resolved the Graham factual inquiries, the proper resolution of which is the requirement for establishing a framework for an objective obviousness analysis. *See* M.P.E.P. § 2141(II), citing to *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), as reiterated by the U.S. Supreme Court in *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398, 82 USPQ2d 1385 (2007). Specifically, as described below, the Final Office Action has not properly ascertained the differences between the claimed invention and the prior art, at least because it has not interpreted the prior art and considered *both* the invention *and* the prior art *as a whole*. See M.P.E.P. § 2141(II)(B).

Independent Claims 24 and 39

The cited references, whether considered alone or in combination, at least do not teach or suggest a "method for cipher-controlled exploitation of data resources stored in a remote database associated with a computer system," which comprises:

> providing a subscriber identity module carrying at least one security algorithm, said subscriber identity module not used by said computer system for communication with a network;
>
> producing a cipher key via said at least one security algorithm;
>
> using said cipher key for protecting said data resources; and
>
> storing said protected data resources in said remote database in an encrypted format,

as recited in claim 24 (emphases added). On page 3, the Final Office Action asserted that Ben discloses all the elements of pending claim 24 except for "a remote storing location accessible by said user," and relied on Campbell to cure the admitted deficiency of Ben. Ben, however, is missing other features as well, and Campbell does not supply those missing features.

As recited in claim 24, a subscriber identification module (SIM) is used for "the cipher controlled exploitation of data resources ... associated with a computer system," which does not use the SIM for communication with a network. Applicant's specification discusses the problem of protecting sensitive and valuable information in a computer system. See, e.g., Applicant's specification at, for example, page 1, lines 15-30. Further, Applicant's specification describes other references in which the SIM of a mobile phone is utilized for logging a user into a computer system, or for generating a copy of a key used in accessing resources. See id. at, for example, page 1, line 31 to page 2, line 32.

Applicant's specification, for example, "aims at providing an arrangement implementing a secure and low-cost method for protecting any sensitive data stored in a computer system and/or a

local access to the computer system itself" (Id. at page 3, lines 6-10, emphases added), and achieves this goal "by means of a SIM (Subscriber Identity Module)" (Id. at lines 11-12). Some arrangements may, for example, take advantage of the existing security functions of a SIM (see, e.g., Id. at lines 21-23) used in a mobile device that can communicate with a mobile network (see, e.g., Id. at page 3, lines 13-20; page 5, lines 31-34), to solve a client security problem of a computer system that is not necessarily associated with that mobile network, and is not using the SIM for its communication with a network (see, e.g., id. at page 5, lines 22-30). Instead the computer system may be interfaced with the SIM through one or more of various technologies, unrelated to the communication of the computer system with a network. See, e.g., id. at page 7, lines 18-28.

Ben, on the other hand, uses a SIM to secure the information on the communication device that uses that SIM for communication with a network. See, e.g., Ben at Abstract. Specifically, Ben is directed to "provid[ing] a device for securing private information associated with the subscriber in a communication apparatus." Ben at column 1, lines 64-65. Further, Ben explains that

> [i]t is am advantage of the present invention that the communication apparatus comprises a cipher-key generating module, such as subscriber information module card, SIM card. The device retrieves the cipher key through the cipher-key generating module to encrypt or decrypt the information associated with the subscriber; therefore, secures the information associated with a subscriber.

Id. at column 2, lines 29-35 (emphasis added).

Campbell is directed to improving wireless devices. Specifically, Campbell attempts to limit the quantity of information stored on wireless devices by uploading some of that information to a remotes server database. See, e.g., Campbell at Abstract.

Therefore, Ben and Campbell are both directed to utilities implemented in a communication device and are concerned with information stored in that communication device.

In particular, Ben utilizes the SIM used by the communication device in its communication with a network. These references do not teach or suggest a "method for cipher-controlled exploitation of data resources stored in a remote database associated with a computer system," which comprises "providing a subscriber identity module [SIM] ... not used by said computer system for communication with a network," and using that SIM for "producing a cipher key ...; using said cipher key for protecting said data resources; and storing said protected data resources ... in an encrypted format," as recited in claim 24. Therefore, at least for the above reasons, claim 24 is not obvious and should be allowable.

Independent claim 39, although differing in scope from claim 24, recites features similar to those discussed above in relation to claim 24. Specifically, claim 39 recites a

> system for cipher-controlled exploitation of data resources, comprising at least one subscriber identity module [SIM] carrying at least one security algorithm; [and] at least one computer system comprising at least one processing module, said subscriber identity module not used by said at least one computer system for communication with a network and said at least one processing module being interfaced with said at least one subscriber identity module to generate a cipher key via said at least one security algorithm and being configured to protect via said cipher key said data resources. (Emphasis added).

Therefore, for at least the reasons stated above in relation to claim 24, claim 39 is also not obvious and should be allowable.

Claim 27

Claim 27 depends from claim 24, and therefore includes features of claim 24 discussed above. Also, claim 27 recites a method which further comprises "generating at least two random values; subjecting said at least two random values to said at least one security algorithm to generate at least two session keys; and combining said at least two session keys via a mixer function to produce said cipher key" (emphases added). In its rejection of claim 27, on page 5,

the Office Action cited column 5, lines 4-15 of Ben. Applicant, however, respectfully notes that the cited section in Ben, or any other section, does not teach or suggest the above features of claim 27. Specifically, the cited section merely describes various modules of a secure device including a random generating module, which, in each operation, generates one random input, used by a cipher-key generating module to generate a cipher key. Ben does not teach or suggest "generating at least two random values ... generat[ing] at least two session keys, ... and combining said at least two session keys via a mixer function to produce [one] cipher key," as recited in claim 27 (emphases added). Therefore, for at least the above reasons, claims 27 is also nonobvious and should be allowable over the cited references.

Claim 29

Claim 29 depends, indirectly, from claim 24, and therefore includes features of claim 24 discussed above. Also, claim 29 recites a method which further comprises "inserting in [a] mixer function a user specific secret unrelated to said subscriber identity module security algorithm, whereby said cipher key is unpredictable even based on knowledge of said security algorithm carried in said subscriber identity module" (emphasis added). Ben does not teach or suggest these features. As an exemplary illustration of these features, Applicant's specification describes an added security measure in which "the mixer function f can include a user specific secret key K_u [in addition to session keys K_c derived as functions of random values] in order to make the encryption key K unpredictable also for the mobile operator, which usually knows the key Ki embedded into the SIM." Applicant's specification, p. 14, lines 32-35 (emphasis added). See also, Applicant's specification at page 10, lines 22-30; page 14 line 32 to page 15, line 2.

In the rejection of claim 29 on page 5, the Office Action cited column 3, lines 28-37 of Ben. However, the cited section merely describes that the cipher-key generating module in Ben

can be a SIM, and that, instead of using a predetermined algorithm in SIM to generate a cipher key, Ben's system can use a previously stored subscriber code, such as International Mobile Subscriber Identity (IMSI) as a cipher key. See Ben column 3, lines 28-37. However, an IMSI can not correspond to the recited user specific secret K_u, because, unlike K_u, IMSI is embedded into the SIM. Moreover, Ben does not teach or suggest that the IMSI, or any user specific secret, is inserted in a mixer function to produce an encryption key, as required by claim 29. Instead, Ben directly uses the IMSI as its cipher key. Therefore, for at least the above reasons, claim 29 is also nonobvious and should be allowable over the cited references.

Claim 34

Claim 34 depends, indirectly, from claim 24, and therefore includes features of claim 24 discussed above. Also, claim 34 recites a method in which "said cryptographic header [of the data in encrypted format] comprises an identifier of said subscriber identity module [SIM] and a cryptographic checksum based on said cipher key, said cryptographic checksum being used for detecting any unauthorized modifications of said encrypted format" (emphasis added). As an exemplary illustration of this feature, Applicant's specification illustrates the cryptographic header and its fields in Fig. 3 and its detailed description.

In its rejection of claim 34 on pages 6-7, the Office Action cited column 5, lines 21-25 of Ben. However, the cited section merely describes that the cipher-key generating module in Ben can be a SIM, and that the predetermined calculating algorithm in Ben can be a HMAC, GSM-A3, or GSM-A8. This section or any other section of Ben does not teach or suggest an encrypted data which includes a cryptographic header comprising a cryptographic checksum, as recited in claim 34. Therefore, for at least the above reasons, claims 34 is also nonobvious and should be allowable over the cited references.

Remaining Claims

Applicant respectfully contends that each of claims 25, 26, 28, 30-33, 35-38, 40, 41, and 43-46 is also nonobvious, at least by virtue of its dependence from one of independent claims 24 and 39, and because they recite additional features not taught or suggested by the cited references. Therefore, claims 25, 26, 28, 30-33, 35-38, 40, 41, and 43-46 should also be allowable over the cited references.

IV. Conclusion

Applicant respectfully requests the reconsideration and withdrawal of the rejections, and the timely allowance of the pending claims.

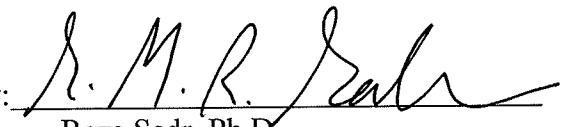
The Final Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statement is identified herein, Applicant declines to automatically subscribe to any statement or characterization in the Final Office Action.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: March 23, 2010

By: 

Reza Sadr, Ph.D.
Reg. No. 63,292

/direct telephone: (617) 452-1563/